Problems with the Linear Cryptanalysis of DES Using more than one Active S-Box per Round

Uwe Blöcher and Markus Dichtl

Siemens AG, ZFE T SN 3, D-81730 München, Germany,
E-Mail:Uwe.Bloecher@zfe.siemens.de or Markus.Dichtl@zfe.siemens.de

Abstract. Matsui introduced the concept of linear cryptanalysis. Originally only one active S-box per round was used. Later he and Biham proposed linear cryptanalysis with more than one active S-box per round. They combine equations with the Piling-up Lemma which requires independent random input variables. This requirement is not met for neighbouring S-boxes, because they share input bits. In this paper we study the error resulting from this application of the Piling-up Lemma. We give statistical evidence that the errors are severe. On the other hand we show that the Piling-up Lemma gives the correct probabilities for Matsui's Type II approximation.

1 Introduction

At Eurocrypt 1993 Matsui [3] introduced linear cryptanalysis. Matsui finds a linear equation in GF(2) between input bits, output bits, and key bits of DES which does not hold in general, but with a probability distinct from 1/2. From a sufficient number of plaintext/ciphertext pairs the attacker can derive information about key bits.

Matsui starts from linear equations for individual S-boxes which hold with a probability disjoint from 1/2. From these equations he derives equations for one round of DES. In the original publication all the bits involved in the equation for a round referred to a single S-box, the active S-box. The equations for the individual rounds have to fit together in such a way that all intermediate bits cancel, and only input bits, output bits and key bits of DES remain. To combine the probabilities of the equations Matsui applies the Piling-up Lemma:

Lemma 1 *Let X_i $(1 \leq i \leq n)$ be independent random variables whose values are in GF(2). Let p_i be the probability that $X_i = 0$. Then the probability that $X_1 + X_2 + \cdots + X_n = 0$ is $1/2 + 2^{(n-1)} \prod_{i=1}^{n} (p_i - 1/2)$.*

At Eurocrypt 1994 both Biham [1] and Matsui [4] presented a generalization of the original attack. Both allowed more than one active S-box per round and combined the equations of the active S-boxes in each round with the Piling-up Lemma. For neighbouring S-boxes this seems to be very questionable, since the Piling-up Lemma requires independent random variables whereas neighbouring

S-boxes share two input bits. As Eli Biham [1] remarks, the Piling-up Lemma holds if we average over all keys. But this is not very useful in an attack, where one wants to find the single fixed key. In this paper we study the error resulting from the application of the Piling-up Lemma on neighbouring S-boxes.

In section 2 we define the notation used. In section 3 we give some examples showing that the Piling-up Lemma gives wrong results. In section 4 we describe how the correct probability for the combination of two equations from neighbouring S-boxes is computed. In section 5 we prove that in some cases, namely for Matsui's Type II approximation, the Piling-up Lemma gives indeed the correct probabilities. In section 5 we study the error resulting from the application of the Piling-up Lemma statistically. We show that errors are frequent and severe. In section 6 conclusions are drawn.

2 Notation

Throughout this paper we use FIPS PUB-46's [5] numbering of DES bits. The input bits, key bits and output bits of the F-function, S-boxes, etc. are numbered from left to right beginning with 1. This numbering is different from Matsui's papers in which he numbers bits from right to left beginning with 0.

We use Matsui's notation in which $A[i]$ represents the i-th bit of A and $A[i_1, i_2, \ldots, i_k]$ is equal to $A[i_1] \oplus A[i_2] \oplus \ldots \oplus A[i_k]$.

We denote by X the input bits, by Y the output bits and by K the key bits of a round.

3 Examples

In this section we give some examples showing the errors resulting from applying the Piling-up Lemma.

Example 1
Combining the equations

$$\begin{aligned} X[4,7,9] \oplus Y[13,18] &= K[7,10,12], \qquad & p = 34/64 \\ X[8,11,12,13] \oplus Y[6,24,30] &= K[13,16,17,18], \qquad & p = 28/64 \end{aligned}$$

from S-boxes S2 and S3 results in

$$X[4,7,8,9,11,12,13] \oplus Y[6,13,18,24,30] = K[7,10,12,13,16,17,18].$$

According to the Piling-up Lemma the resulting equation has probability 0.496. But there is no key for which this probability is correct! The correct probabilities for the four essentially distinct classes of keys (cf. section 4) are:

Keys	Probability
$K[11] = K[13]$ and $K[12] = K[14]$	0.461
$K[11] = K[13]$ and $K[12] \neq K[14]$	0.508
$K[11] \neq K[13]$ and $K[12] = K[14]$	0.508
$K[11] \neq K[13]$ and $K[12] \neq K[14]$	0.508

For the class of keys with probability 0.461 (25% of the keys) linear cryptanalysis will find the right key bit, because 0.461 and the Piling-up value 0.496 are on the same side of 1/2. For the remaining 75% of the keys Matsui's algorithm 1 for linear cryptanalysis will determine a wrong key bit.

Example 2
If we combine the following equations from the S-boxes S8 and S7

$$\begin{aligned} X[1,28,30,32] \oplus Y[5] &= K[43,45,47,48], \quad && p = 24/64 \\ X[27,29] \oplus Y[7,12,22,32] &= K[40,42], && p = 42/64 \end{aligned}$$

we get the resulting equation

$$X[1,27,28,29,30,32] \oplus Y[5,7,12,22,42] = K[40,42,43,45,47,48].$$

According to the Piling-up Lemma the resulting equation has probability 0.461. But the correct probabilities for the four classes of keys are:

Keys	Probability
$K[41] = K[43]$ and $K[42] = K[44]$	0.445
$K[41] = K[43]$ and $K[42] \neq K[44]$	0.469
$K[41] \neq K[43]$ and $K[42] = K[44]$	0.430
$K[41] \neq K[43]$ and $K[42] \neq K[44]$	1/2

For 25% of the keys the probability is 1/2. For these keys linear cryptanalysis will give no information about the key bits.

Example 3
Combining the equations

$$\begin{aligned} X[4] \oplus Y[9,17,31] &= K[5], \quad && p = 30/64 \\ X[4] \oplus Y[2,18,28] &= K[7], && p = 32/64 = 1/2 \end{aligned}$$

from the S-boxes S1 and S2 results in

$$Y[2,9,17,18,28,31] = K[5,7].$$

Because the probability of one equation is 1/2 the resulting equation must have probability 1/2 according to the Piling-up Lemma! But the actual probabilities for the four classes of keys are:

Keys	Probability
$K[5] = K[7]$ and $K[6] = K[8]$	0.512
$K[5] = K[7]$ and $K[6] \neq K[8]$	0.488
$K[5] \neq K[7]$ and $K[6] = K[8]$	0.512
$K[5] \neq K[7]$ and $K[6] \neq K[8]$	0.488

Example 3 shows that it is probably not sufficient to restrict linear cryptanalysis to those equations for one S-box which have probability unequal to 1/2.

Example 4
Combining the equations

$$X[1,4] \oplus Y[9,17,23,31] = K[5], \qquad p = 22/64$$
$$X[4,5,6,7,8,9] \oplus Y[13] = K[7,8,9,10,11,12], \qquad p = 30/64$$

from the S-boxes S1 and S2 results in

$$X[1,5,6,7,8,9] \oplus Y[9,13,17,23,31] = K[5,7,8,9,10,11,12].$$

According to the Piling-up Lemma the resulting equation has probability 0.5098. But the correct probabilities for the four classes of keys are:

Keys	Probability
$K[5] = K[7]$ and $K[6] = K[8]$	0.375000
$K[5] = K[7]$ and $K[6] \neq K[8]$	0.656250
$K[5] \neq K[7]$ and $K[6] = K[8]$	0.398438
$K[5] \neq K[7]$ and $K[6] \neq K[8]$	0.609375

These probabilities deviate largely from the Piling-up probability.

4 How to find the correct probabilities for a given key

In this paper we restrict ourselves to two active S-boxes per round. We state that for a given key the combination of two equations of neighbouring S-boxes in one round with the Piling-up Lemma often gives a wrong probability. The correct probability for a given key can be computed if we regard two neighbouring DES S-boxes as one bigger S-box. The expansion mapping E, the permutation P and the round key bits are taken into account. The bigger S-box therefore has 8 output bits and 10 input bits (2 of them are doubled), which are xored with 12 round key bits. Figure 1 shows the S-box combined of S1 and S2.

For a given equation and given round key bits the probability can be computed by testing all 2^{10} inputs and counting the number of inputs for which the equation holds. The fast Walsh Transform can be used to speed up this computation.

It is obvious that only the four round key bits which are xored to the doubled input bits can affect the probability. (The other key bits only change the order of counting.) These four round key bits decide whether the doubled input bits remain equal after xoring the round key or not. So we have four classes of round keys.

5 A case for which the Piling-up Lemma holds

The following theorem shows that the Piling-up Lemma gives the correct probability for Matsui's Type II approximation of DES ([4], [2]). Matsui gives the example where the two equations from S7 and S8

$$X[28,29] \oplus Y[7,12,22,32] = K[41,42], \qquad p = 40/64$$
$$X[28,29] \oplus Y[5,21,27] = K[43,44], \qquad p = 20/64$$

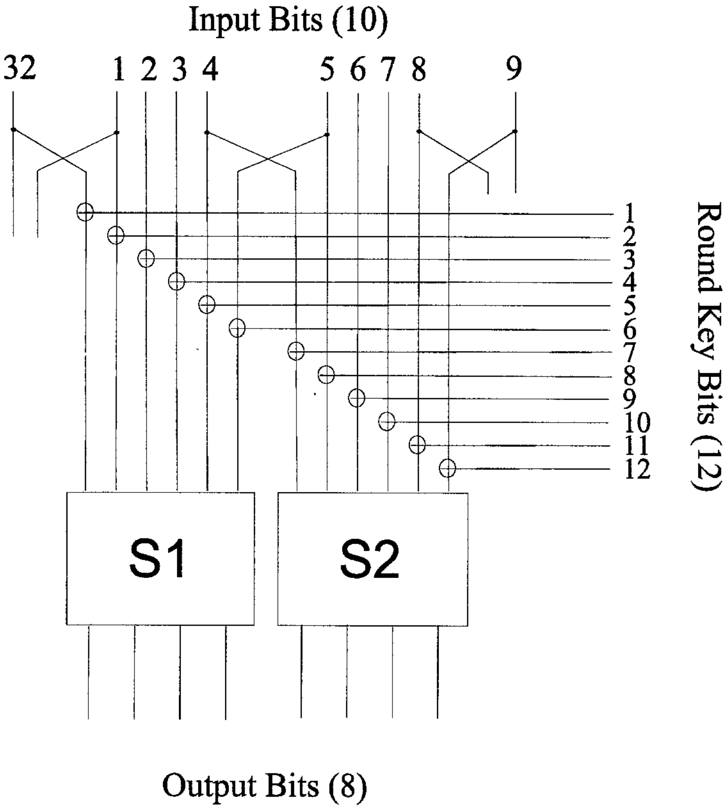

Fig. 1. Combined S-box of S1 and S2.

are combined to the equation

$$Y[5,7,12,21,22,27,32] = K[41,42,43,44].$$

in which all input bits are cancelled out. The probability 0.453 computed with the Piling-up Lemma is correct for all keys.

Theorem 1 *Let E_1 and E_2 be linear equations for adjoining DES S-boxes. Let E_1 and E_2 be such that the two input bits of the DES F-function which go to both S-boxes are terms of both equations, and that no other input bits are used in the equations. Let p_i be the probability of equation E_i (i=1,2). Then for each value of the round key the probability of the combined equation of E_1 and E_2 is $\frac{1}{2} + 2 \cdot (p_1 - \frac{1}{2}) \cdot (p_2 - \frac{1}{2})$, the Piling-up Lemma can be applied.*

Proof of Theorem 1: Let B_1 and B_2 be two adjoining DES S-Boxes. Let $b_{i1}, \ldots, b_{i6}$ be the input bits of B_i $(i = 1,2)$. Let $y_{i1}, \ldots, y_{i4}$ be the output bits of B_i $(i = 1,2)$. We have $b_{11} = k_1 + x_1$, $b_{12} = k_2 + x_2$, $b_{13} = k_3 + x_3$,

$b_{14} = k_4 + x_4$, $b_{15} = k_5 + x_5$, $b_{16} = k_6 + x_6$, $b_{21} = k_7 + x_5$, $b_{22} = k_8 + x_6$, $b_{23} = k_9 + x_7$, $b_{24} = k_{10} + x_8$, $b_{25} = k_{11} + x_9$, $b_{26} = k_{12} + x_{10}$. The k_j are key bits, the x_j are input bits of the F-function.

We consider the two equations

$$x_5 + x_6 + \sum_{i \epsilon I_1} y_{1i} = k_5 + k_6$$

and

$$x_5 + x_6 + \sum_{i \epsilon I_2} y_{2i} = k_7 + k_8$$

with $I_1 \subseteq \{1, \ldots, 4\}$ and $I_2 \subseteq \{5, \ldots, 8\}$

We prove that the number of 10-tuples $(x_1, \ldots, x_{10})$ for which the combined equation

$$\sum_{i \epsilon I_1} y_{1i} + \sum_{i \epsilon I_2} y_{2i} = k_5 + k_6 + k_7 + k_8 \tag{1}$$

holds does not depend on the values of k_5, k_6, k_7, and k_8.

The Piling-up Lemma gives the probability of the combined equation averaged over all possible (k_5, k_6, k_7, k_8). When the probability does not depend on the key bits, the Piling-up Lemma gives a correct result also for fixed key bits.

We prove now that changing the key bit k_5 does not change the number of 10-tuples $(x_1, \ldots, x_{10})$ for which equation (1) holds.

We have to consider the 10-tuples for which $\sum_{i \epsilon I_1} y_{1i} + \sum_{i \epsilon I_2} y_{2i}$ does not change when k_5 is toggled. In these cases $\sum_{i \epsilon I_1} y_{1i}$ does not depend on k_5. Each of those 10-tuples falls into one of two classes:

Class A : Those 10-tuples for which $\sum_{i \epsilon I_2} y_{2i}$ does not depend on the key bit k_7. Then for one of the 10-tuples $(x_1, \ldots, x_4, x_5, x_6 \ldots, x_{10})$ and $(x_1, \ldots, x_4, 1 + x_5, x_6 \ldots, x_{10})$ the sum $\sum_{i \epsilon I_1} y_{1i} + \sum_{i \epsilon I_2} y_{2i}$ takes the value 0 , and for the other 10-tuple the value 1 is taken.

Class B : Those 10-tuples for which $\sum_{i \epsilon I_2} y_{2i}$ depends on the key bit k_7. Here we make use of the special form of DES S-boxes, namely that the input bits b_1 and b_6 select from four permutations. As a consequence $\sum_{i \epsilon I_1} y_{1i}$ takes as many zeros as ones when we consider as inputs all the 10-tuples $(x_1, \ldots, x_{10})$ where $x_1, \ldots, x_5$ run through all possible 2^5 values whereas $x_6, \ldots x_{10}$ remain fixed. As a consequence of the balanced zeros and ones for each pair of such 10-tuples $(x_1, \ldots, x_4, x_5, x_6, \ldots, x_{10})$ and $(x_1, \ldots, x_4, 1 + x_5, x_6, \ldots x_{10})$ where $\sum_{i \epsilon I_1} y_{1i}$ takes the value z for both, there is another pair $(x'_1, \ldots, x'_4, x'_5, x_6, \ldots x_{10})$ and $(x'_1, \ldots, x'_4, 1 + x'_5, x_6, \ldots x_{10})$ where the sum takes the value 1+z for both.

In both classes there are as many 10-tuples $(x_1, \ldots, x_{10})$ where $\sum_{i \epsilon I_1} y_{1i} + \sum_{i \epsilon I_2} y_{2i}$ takes the value 0 as there are with the value 1. So the number of those 10-tuples for which equation 1 holds does not change when k_5 is toggled.

The argument for k_7 is very similar, k_6 and k_8 follow by symmetry. □

6 Statistics

We compare the probabilities given by the Piling up Lemma to the correct ones which were computed as described in section 4. When they are different, three things can happen:

a) We may get wrong key bits from the attack. This happens when the computed probability and the actual probability for the key are on different sides of 1/2.
b) We may get no information at all. This happens when the actual probability for the key is equal to 1/2.
c) Our estimations of the number of plaintext ciphertext pairs required for the attack may be wrong.

We studied the effects a), b), and c) statistically. We started from the set of all 5507 equations for single DES S-boxes with probability distinct from 1/2 and 1. We considered pairs of such equations which refer to neighbouring S-boxes. (Of course the S-boxes S1 and S8 are considered as neighbouring.) We took a random sample of 1000 from these pairs. For each pair there are four essentially different types of round keys.

For each type of round key we computed the probability of the combined equation. So we had 4000 cases for comparing the correct probability and the probability from the application of the Piling-up Lemma.

The results are shown in table 1.

Case	Percentage
Piling-up Lemma holds	14.1%
a) Wrong key bits	22.2%
b) No information	9.8%
c) Wrong estimation of number of plain-/ciphertext pairs	54.0%

Table 1. Statistics of 1000 samples of equations referring to neighbouring S-boxes. The equations were chosen from all 5507 equations.

The Piling-up Lemma gave the correct result in 562 cases, which makes 14.1% of 4000. 886 cases or 22.2% belong to case a), an attacker which relies on the Piling-up Lemma will get wrong key bits. 393 cases or 9.8% belong to case b), the attacker does not get information.

For the 2721 cases which do not belong to a) or b) the deviation of the result computed by the Piling-up Lemma from the correct value was analysed. The number of plaintext/ciphertext pairs required for linear cryptanalysis is proportional to $(p - 1/2)^{-2}$ where p is the probability of the equation used for the attack. We use p_l to denote probabilities computed with the Piling-up

Lemma and p_c for the correct probabilities. The work factor $f = \frac{(p_l-1/2)^{-2}}{(p_c-1/2)^{-2}}$ is the factor by which the number of plaintext/ciphertext pairs according to the Piling-up Lemma deviates from the correct value. In 20% of the the cases f is above 10, linear cryptanalysis in these cases is more than an order of magnitude easier than suggested by the Piling-up Lemma. For 53% of the cases, f is above 2. For 12% of the cases f is below 0.5. Figure 2 shows the distribution of f.

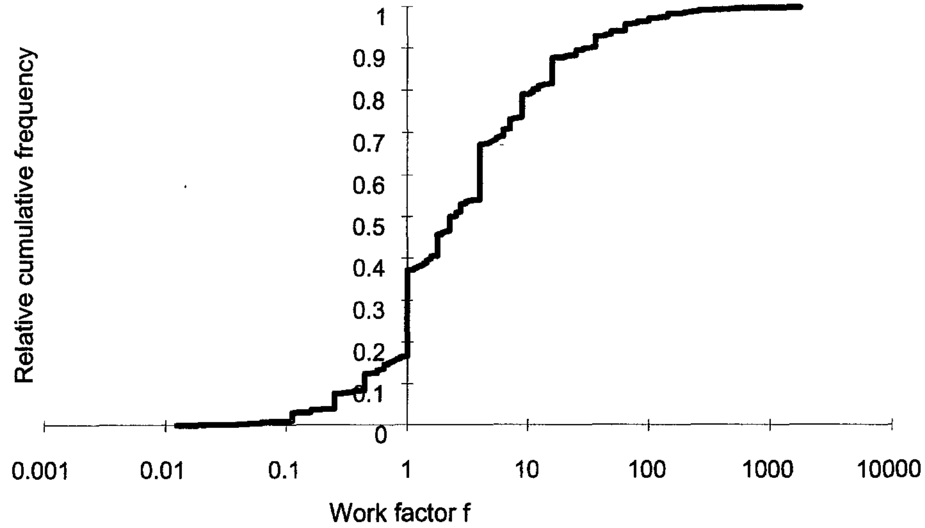

Fig. 2. Relative error in the number of required plaintext/ciphertext pairs caused by the Piling-up Lemma for all equations.

The effect of the Piling-up Lemma on "good" equations was also studied. Of course "good" equations are preferable for the attack, but in order to find equation which fit, one has to accept "bad" ones as well. The best set of equations for the linear cryptanalysis of DES [3] contains three times an equation with probability 30/64, the worst probability possible.

For the "good" equations we used the same method as above, but took only those equations for whose probabilities p holds $| p - 1/2 | \geq 8/64$. These 669 are the best 12% of the equations. Again we considered 1000 pairs of equations from neighbouring S-boxes, which makes 4000 cases.

The results are shown in table 2.

The Piling-up Lemma gave the correct result in 901 cases, which makes 22.5% of 4000. 37 cases or 0.9% belong to case a), an attacker which relies on the Piling-up Lemma will get wrong key bits. 19 cases or 0.4% belong to case b), the attacker does not get information.

Case	Percentage
Piling-up Lemma holds	22.5%
a) Wrong key bits	0.9%
b) No information	0.4%
c) Wrong estimation of number of plain-/ciphertext pairs	76.1%

Table 2. Statistics of 1000 samples of equations referring to neighbouring S-boxes. The equations were chosen from the best 12% of the equations.

For the 3944 cases which do not belong to a) or b) the distribution of f was studied. For 9.4% of the cases f is above 2. For 14% of the cases f is below 0.5. For 2.7% of the cases f is below 0.1. Figure 3 shows the distribution of f.

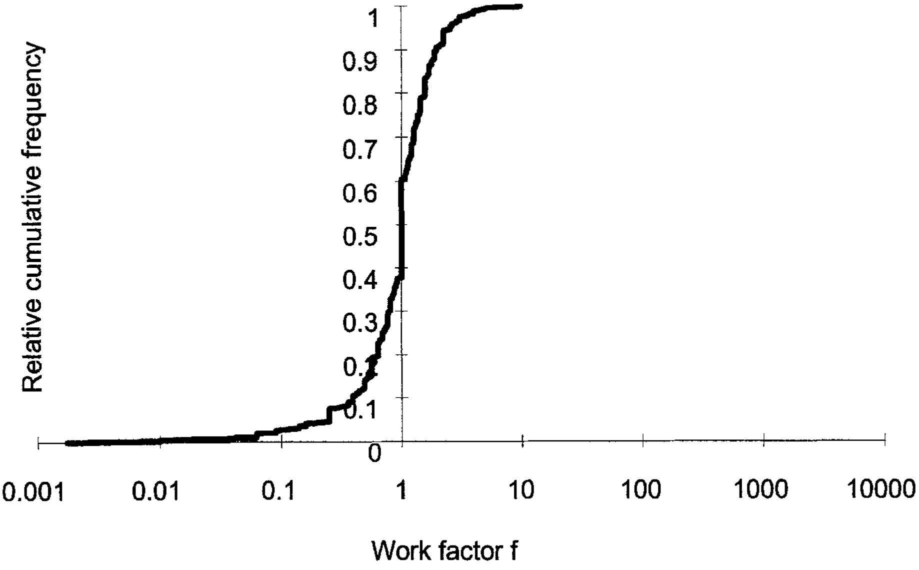

Fig. 3. Relative error in the number of required plaintext/ciphertext pairs caused by the Piling-up Lemma for the best 12% of the equations.

7 Conclusions

We have shown that the extension of Matsui's linear cryptanalysis as suggested by Matsui and Biham does not have a sound theoretical basis. Our statistical results suggest that this method leads to significant errors in practical attacks. This goes as far as the computation of wrong key bits.

On the other hand we have proved that Matsui' s approximations of Type II are valid for DES under the assumption of independent round keys.

But in general, the extension of linear cryptanalysis to more than one active S-box per round has, to the best of our knowledge, to be considered as an open problem.

References

1. Eli Biham. On Matsui's linear cryptanalysis. In *Pre-proceedings of Eurocrypt '94*, pages 349 – 361, 1994.
2. Mitsuru Matsui. Linear cryptanalysis of DES cipher (I) (Version 1.03). Preprint.
3. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - Eurocrypt '93*, number 765 in Lecture Notes in Computer Science, pages 386 – 397. Springer-Verlag, 1993.
4. Mitsuru Matsui. On correlation between the order of S-boxes and the strength of DES. In *Pre-proceedings of Eurocrypt '94*, pages 377 – 387, 1994.
5. National Bureau of Standards. Data Encryption Standard. FIPS Publ. 46, Washington, DC, 1977.